PCT/EP2003/010015

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference CPCT-12366	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP2003/010015	International filing date (*day/month/year*) 09 September 2003 (09.09.2003)	Priority date (*day/month/year*) 11 September 2002 (11.09.2002)
International Patent Classification (IPC) or national classification and IPC H04L 9/30		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
02 March 2004 (02.03.2004)	14 December 2004 (14.12.2004)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP2003/010015

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-19, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-13, filed with the letter of 07 September 2004 (07.09.2004)

☒ the drawings:

pages 1/4-4/4, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17)*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP 03/10015	International filing date (day/month /year)	Priority date (day/month/year)
International Patent Classification (IPC) or national classification and IPC		
Applicant		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of _____ sheets, including this cover sheet.

   [X] This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I [X] Basis of the report
   - II [ ] Priority
   - III [ ] Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV [ ] Lack of unity of the invention
   - V [X] Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability: citations and explanations supporting such statement
   - VI [ ] Certain documents cited
   - VII [ ] Certain defects in the international application
   - VIII [ ] Certain observations on the international application

Date of submission of the demand	Date of completion of this report
Name and mailing address of the IPEA/ Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP 03/10015

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-13	YES
	Claims		NO
Inventive step (IS)	Claims	1-13	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-13	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following document:

D1: WO 01/61918 (SILVERBROOK RES PTY LTD; WALMSLEY SIMON ROBERT (AU); LAPSTUN PAUL), 23 August 2001 (2001-08-23)

1. Document D1, which is considered to be the prior art closest to the subject matter of claim 1, discloses a method for the protected execution of a cryptographic calculation using a key with at least two key parameters (page 69, line 4, "K_1" and "K_2"), and involving a key integrity check (page 69, lines 4 to 9) to prevent a cryptographic attack in which corruption of at least one first key parameter allows conclusions to be drawn about at least one second key parameter.

The subject matter of claim 1 differs from the known method in that at least one key parameter is the product of a value required for the cryptographic calculation and a security value, and in that the integrity check includes a divisibility check.

The subject matter of claim 1 is therefore novel (PCT Article 33(2)).

The problem addressed by the present invention can thus be seen as that of avoiding the multiple execution of the elaborate calculation of the HMAC-SHA1 checksum in D1.

The solution proposed in claim 1 of the present application involves an inventive step (PCT Article 33(3)) because the problem of avoiding the compute-bound HMAC-SHA1 checksum calculation is not even hinted at in D1. D1 does not state that at least one key parameter is the product of a value required for the cryptographic calculation and a security value, or that the integrity check includes a divisibility check. There is also no suggestion of this type of integrity check, even though such a check avoids the need for the compute-bound HMAC-SHA1 checksum calculation since the mathematical relations inherent in the key parameters and security values are used, so that for the purposes of the integrity check a divisibility check will suffice instead of the checksum calculation.

2. The above comments apply accordingly to independent claims 12 and 13, which relate, respectively, to a computer program product and a chip card for executing the method of claim 1. Claims 12 and 13 are therefore also novel (PCT Article 33(2)) and inventive (PCT Article 33(3)).

3. Claims 2 to 11 are dependent on claim 1 and therefore also meet the PCT requirements in respect of novelty and inventive step.